(8) Establish administrative processes in WHS-Serviced Component organizations to comply with the procedures listed in this part and 32 CFR part 310.

(9) Coordinate with WHS General Counsel on all proposed denials of access to records.

(10) Provide justification to the OSD/JS Privacy Office when access to a record is denied in whole or in part.

(11) Provide the record to the OSD/JS Privacy Office when the initial denial of a request for access to such record has been appealed by the requester or at the time of initial denial if an appeal seems likely.

(12) Maintain an accurate administrative record documenting the actions resulting in a denial for access to a record or for the correction of a record. The administrative record should be maintained so it can be relied upon and submitted as a complete record of proceedings if litigation occurs in accordance with 32 CFR part 310.

(13) Ensure all personnel are aware of the requirement to take appropriate Privacy Act training as required by 32 CFR part 310 and the Privacy Act.

(14) Forward all requests for access to records received directly from an individual to the OSD/JS Freedom of Information Act Requester Service Center for processing under 32 CFR part 310 and 32 CFR part 286.

(15) Maintain a record of each disclosure of information (other than routine use) from a system of records as required by 32 CFR part 310.

§311.6 Procedures.

(a) *Publication of Notice in the* FEDERAL REGISTER. (1) A notice shall be published in the FEDERAL REGISTER of any record system meeting the definition of a system of records in 32 CFR 310.4.

(2) The Heads of the WHS-Serviced Component shall submit notices for new or revised systems of records to the Chief, OSD/JS Privacy Office, for review at least 90 days prior to desired implementation.

(3) The Chief, OSD/JS Privacy Office shall forward completed notices to the Defense Privacy Office (DPO) for review in accordance with 32 CFR 310.30. Publication in the FEDERAL REGISTER starts a 30-day comment window which provides the public with an opportunity to submit written data, views, or arguments to the DPO for consideration before a system of record is established or modified.

(b) *Access to Systems of Records Information*. (1) As provided in the Privacy Act, records shall be disclosed only to the individual they pertain to and under whose individual name or identifier they are filed, unless exempted by the provisions in 32 CFR 310.31. If an individual is accompanied by a third party, the individual shall be required to furnish a signed access authorization granting the third party access according to 32 CFR 310.17.

(2) Individuals seeking access to records that pertain to themselves, and that are filed by name or other personal identifier, may submit the request in person or by mail, in accordance with these procedures:

(i) Any individual making a request for access to records in person shall provide personal identification to the appropriate system owner, as identified in the system of records notice published in the FEDERAL REGISTER, to verify the individual's identity according to 32 CFR 310.17.

(ii) Any individual making a request for access to records by mail shall address such request to the OSD/JS FOIA Requester Service Center, Office of Freedom of Information, 1155 Pentagon, Washington, DC 20301–1155. To verify his or her identity, the requester shall include either a signed notarized statement or an unsworn declaration in the format specified by 32 CFR part 286.

(iii) All requests for records shall describe the record sought and provide sufficient information to enable the material to be located (*e.g.*, identification of system of records, approximate date it was initiated, originating organization, and type of document).

(iv) All requesters shall comply with the procedures in 32 CFR part 310 for inspecting and/or obtaining copies of requested records.

(v) If the requester is not satisfied with the response, he or she may file a written appeal as provided in paragraph (f)(8) of this section. The requester must provide proof of identity

by showing a driver's license or similar credentials.

(3) There is no requirement that an individual be given access to records that are not in a group of records that meet the definition of a system of records in the Privacy Act. (For an explanation of the relationship between the Privacy Act and the Freedom of Information Act, and for guidelines to ensure requesters are given the maximum amount of information authorized by both Acts, *see* 32 CFR part 310.17

(4) Granting access to a record containing personal information shall not be conditioned upon any requirement that the individual state a reason or otherwise justify the need to gain access.

(5) No verification of identity shall be required of an individual seeking access to records that are otherwise available to the public.

(6) Individuals shall not be denied access to a record in a system of records about themselves because those records are exempted from disclosure under 32 CFR part 286. Individuals may only be denied access to a record in a system of records about themselves when those records are exempted from the access provisions of 32 CFR 310.26.

(7) Individuals shall not be denied access to their records for refusing to disclose their Social Security Number (SSN), unless disclosure of the SSN is required by statute, by regulation adopted before January 1, 1975, or if the record's filing identifier and only means of retrieval is by SSN (Privacy Act, note).

(c) *Access to Records or Information Compiled for Law Enforcement Purposes.*

(1) Requests are processed under 32 CFR part 310 and 32 CFR part 286 to give requesters a greater degree of access to records on themselves.

(2) Records (including those in the custody of law enforcement activities) that have been incorporated into a system of records exempted from the access conditions of 32 CFR part 310, will be processed in accordance with 32 CFR 286.12. Individuals shall not be denied access to records solely because they are in the exempt system. They will have the same access that they would receive under 32 CFR part 286. (*See also* 32 CFR 310.17.)

(3) Records systems exempted from access conditions will be processed under 32 CFR 310.26 or 32 CFR 286.12, depending upon which regulation gives the greater degree of access. (*See also* 32 CFR 310.17.)

(4) Records systems exempted from access under 32 CFR 310.27 that are temporarily in the hands of a non-law enforcement element for adjudicative or personnel actions, shall be referred to the originating agency. The requester will be informed in writing of this referral.

(d) *Access to Illegible, Incomplete, or Partially Exempt Records.* (1) An individual shall not be denied access to a record or a copy of a record solely because the physical condition or format of the record does not make it readily available (*e.g.*, deteriorated state or on magnetic tape). The document will be prepared as an extract, or it will be exactly recopied.

(2) If a portion of the record contains information that is exempt from access, an extract or summary containing all of the information in the record that is releasable shall be prepared.

(3) When the physical condition of the record makes it necessary to prepare an extract for release, the extract shall be prepared so that the requester will understand it.

(4) The requester shall be informed of all deletions or changes to records.

(e) *Access to Medical Records.* (1) Medical records shall be disclosed to the individual and may be transmitted to a medical doctor named by the individual concerned.

(2) The individual may be charged reproduction fees for copies or records as outlined in 32 CFR 310.20.

(f) *Amending and Disputing Personal Information in Systems of Records.*

(1) The Head of a WHS-Serviced Component, or designated official, shall allow individuals to request amendment to their records to the extent that such records are not accurate, relevant, timely, or complete.

(2) Requests shall be submitted in person or by mail to the office designated in the system of records notice. They should contain, as a minimum, identifying information to locate the record, a description of the items to be

amended, and the reason for the change. Requesters shall be required to provide verification of their identity as stated in paragraphs (b)(2)(i) and (b)(2)(ii) of this section to ensure that they are seeking to amend records about themselves and not, inadvertently or intentionally, the records of others.

(3) Requests shall not be rejected nor required to be resubmitted unless additional information is essential to process the request.

(4) The appropriate system manager shall mail a written acknowledgment to an individual's request to amend a record within 10 workdays after receipt. Such acknowledgment shall identify the request and may, if necessary, request any additional information needed to make a determination. No acknowledgment is necessary if the request can be reviewed and processed and if the individual can be notified of compliance or denial within the 10-day period. Whenever practical, the decision shall be made within 30 working days. For requests presented in person, written acknowledgment may be provided at the time the request is presented.

(5) The Head of a WHS-Serviced Component, or designated official, shall promptly take one of three actions on requests to amend the records:

(i) If the WHS-Serviced Component official agrees with any portion or all of an individual's request, he or she will proceed to amend the records in accordance with existing statutes, regulations, or administrative procedures and inform the requester of the action taken in accordance with 32 CFR 310.19. The WHS-Serviced Component official shall also notify all previous holders of the record that the amendment has been made and shall explain the substance of the correction.

(ii) If the WHS-Serviced Component official disagrees with all or any portion of a request, the individual shall be informed promptly of the refusal to amend a record, the reason for the refusal, and the procedure to submit an appeal as described in paragraph (f)(8) of this section.

(iii) If the request for an amendment pertains to a record controlled and maintained by another Federal agency, the request shall be referred to the appropriate agency and the requester advised of this.

(6) When personal information has been disputed by the requestor, the Head of a WHS-Serviced Component, or designated official, shall:

(i) Determine whether the requester has adequately supported his or her claim that the record is inaccurate, irrelevant, untimely, or incomplete.

(ii) Limit the review of a record to those items of information that clearly bear on any determination to amend the record, and shall ensure that all those elements are present before a determination is made.

(7) If the Head of a WHS-Serviced Component, or designated official, after an initial review of a request to amend a record, disagrees with all or any portion of the request to amend a record, he or she shall:

(i) Advise the individual of the denial and the reason for it.

(ii) Inform the individual that he or she may appeal the denial.

(iii) Describe the procedures for appealing the denial, including the name and address of the official to whom the appeal should be directed. The procedures should be as brief and simple as possible.

(iv) Furnish a copy of the justification of any denial to amend a record to the OSD/JS Privacy Office.

(8) If an individual disagrees with the initial WHS-Serviced Component determination, he or she may file an appeal. If the record is created and maintained by a WHS-Serviced Component, the appeal should be sent to the Chief, OSD/JS Privacy Office, WHS, 1155 Defense Pentagon, Washington, DC 20301–1155.

(9) If, after review, the Chief, OSD/JS Privacy Office, determines the system of records should not be amended as requested, the Chief, OSD/JS Privacy Office, shall provide a copy of any statement of disagreement to the extent that disclosure accounting is maintained in accordance with 32 CFR 310.25 and shall advise the individual:

(i) Of the reason and authority for the denial.

(ii) Of his or her right to file a statement of the reason for disagreeing with the OSD/JS Privacy Office's decision.

(iii) Of the procedures for filing a statement of disagreement.

(iv) That the statement filed shall be made available to anyone the record is disclosed to, together with a brief statement by the WHS-Serviced Component summarizing its reasons for refusing to amend the records.

(10) If the Chief, OSD/JS Privacy Office, determines that the record should be amended in accordance with the individual's request, the WHS-Serviced Component shall amend the record, advise the individual, and inform previous recipients where a disclosure accounting has been maintained in accordance with 32 CFR 310.25.

(11) All appeals should be processed within 30 workdays after receipt by the proper office. If the Chief, OSD/JS Privacy Office, determines that a fair and equitable review cannot be made within that time, the individual shall be informed in writing of the reasons for the delay and of the approximate date the review is expected to be completed.

(g) *Disclosure of Disputed Information.* (1) If the OSD/JS Privacy Office determines the record should not be amended and the individual has filed a statement of disagreement under paragraph (f)(8) of this section, the WHS-Serviced Component shall annotate the disputed record so it is apparent to any person to whom the record is disclosed that a statement has been filed. Where feasible, the notation itself shall be integral to the record. Where disclosure accounting has been made, the WHS-Serviced Component shall advise previous recipients that the record has been disputed and shall provide a copy of the individual's statement of disagreement in accordance with 32 CFR 310.21.

(i) This statement shall be maintained to permit ready retrieval whenever the disputed portion of the record is disclosed.

(ii) When information that is the subject of a statement of disagreement is subsequently disclosed, the WHS-Serviced Component designated official shall note which information is disputed and provide a copy of the individual's statement.

(2) The WHS-Serviced Component shall include a brief summary of its reasons for not making a correction when disclosing disputed information. Such statement shall normally be limited to the reasons given to the individual for not amending the record.

(3) Copies of the WHS-Serviced Component summary will be treated as part of the individual's record; however, it will not be subject to the amendment procedure outlined in paragraph (f) of this section.

(h) *Penalties.* (1) *Civil Action.* An individual may file a civil suit against the WHS-Serviced Component or its employees if the individual feels certain provisions of the Privacy Act have been violated.

(2) *Criminal Action.* (i) Criminal penalties may be imposed against an officer or employee of a WHS-Serviced Component for these offenses listed in the Privacy Act:

(A) Willful unauthorized disclosure of protected information in the records;

(B) Failure to publish a notice of the existence of a record system in the FEDERAL REGISTER; and

(C) Requesting or gaining access to the individual's record under false pretenses.

(ii) An officer or employee of a WHS-Serviced Component may be fined up to $5,000 for a violation as outlined in paragraphs (h)(2)(i)(A) through (h)(2)(i)(C) of this section.

(i) *Litigation Status Sheet.* Whenever a complaint citing the Privacy Act is filed in a U.S. District Court against the Department of Defense, a WHS-Serviced Component, or any employee of a WHS-Serviced Component, the responsible system manager shall promptly notify the OSD/JS Privacy Office, which shall notify the DPO. The litigation status sheet in Appendix H of 32 CFR part 310 provides a standard format for this notification. (The initial litigation status sheet shall, as a minimum, provide the information required by items 1 through 6). A revised litigation status sheet shall be provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the judgment or opinion shall be provided to the OSD/JS Privacy Office with the litigation status sheet reporting that judgment or opinion.

(j) *Computer Matching Programs.* 32 CFR 310.52 prescribes that all requests

for participation in a matching program (either as a matching agency or a source agency) be submitted to the DPO for review and compliance. The WHS-Serviced Components shall submit a courtesy copy to the OSD/JS Privacy Office at the time of transmittal to the DPO.

§ 311.7 OSD/JS Privacy Office Processes.

The OSD/JS Privacy Office shall:

(a) Exercise oversight and administrative control of the OSD/JS Privacy Program for the WHS-Serviced Components.

(b) Provide guidance and training to the WHS-Serviced Components as required by 32 CFR 310.37.

(c) Collect and consolidate data from the WHS-Serviced Components and submit reports to the DPO, as required by 32 CFR 310.40 or otherwise requested by the DPO.

(d) Coordinate and consolidate information for reporting all record systems, as well as changes to approved systems, to the DPO for final processing to the Office of Management and Budget, the Congress, and the FEDERAL REGISTER, as required by 32 CFR part 310.

(e) In coordination with DPO, serve as the appellate authority for the WHS-Serviced Components when a requester appeals a denial for access as well as when a requester appeals a denial for amendment or initiates legal action to correct a record.

(f) Refer all matters about amendments of records and general and specific exemptions under 32 CFR 310.19, 310.28 and 310.29 to the proper WHS-Serviced Components.

§ 311.8 Procedures for exemptions.

(a) *General information*. The Secretary of Defense designates those Office of the Secretary of Defense (OSD) systems of records which will be exempt from certain provisions of the Privacy Act. There are two types of exemptions, general and specific. The general exemption authorizes the exemption of a system of records from all but a few requirements of the Act. The specific exemption authorizes exemption of a system of records or portion thereof, from only a few specific requirements. If an OSD Component originates a new system of records for which it proposes an exemption, or if it proposes an additional or new exemption for an existing system of records, it shall submit the recommended exemption with the records system notice as outlined in § 311.6. No exemption of a system of records shall be considered automatic for all records in the system. The systems manager shall review each requested record and apply the exemptions only when this will serve significant and legitimate Government purpose.

(b) *General exemptions*. The general exemption provided by 5 U.S.C. 552a(j)(2) may be invoked for protection of systems of records maintained by law enforcement activities. Certain functional records of such activities are not subject to access provisions of the Privacy Act of 1974. Records identifying criminal offenders and alleged offenders consisting of identifying data and notations of arrests, the type and disposition of criminal charges, sentencing, confinement, release, parole, and probation status of individuals are protected from disclosure. Other records and reports compiled during criminal investigations, as well as any other records developed at any stage of the criminal law enforcement process from arrest to indictment through the final release from parole supervision are excluded from release.

(1) *System identifier and name:* DWHS P42.0, DPS Incident Reporting and Investigations Case Files.

(i) *Exemption*. Portions of this system that fall within 5 U.S.C. 552a(j)(2) are exempt from the following provisions of 5 U.S.C. 552a, Sections (c)(3) and (4); (d)(1) through (d)(5); (e)(1) through (e)(3); (e)(5); (f)(1) through (f)(5); (g)(1) through (g)(5); and (h) of the Act.

(ii) *Authority:* 5 U.S.C. 552a(j)(2).

(iii) *Reason:* The Defense Protective Service is the law enforcement body for the jurisdiction of the Pentagon and immediate environs. The nature of certain records created and maintained by the DPS requires exemption from access provisions of the Privacy Act of 1974. The general exemption, 5 U.S.C. 552a(j)(2), is invoked to protect ongoing